Finite Fields and Their Applications **6,** 175–191 (2000)
doi:10.1006/ffta.1999.0270, available online at http://www.idealibrary.com on IDEAL®

Rings of Low Multiplicative Complexity

Joseph H. Silverman

Mathematics Department, Box 1917, Brown University, Providence, Rhode Island 02912
E-Mail: jhs@math.brown.edu

Communicated by Peter Jau-Shyong Shiue

Received September 21, 1999

The complexity of the multiplication operation in finite fields is of interest for both theoretical and practical reasons. For example, an optimal normal basis for $\mathbb{F}_{2^N}$ has complexity $2N-1$. A construction described in J. H. Silverman, ("Cryptographic Hardware and Embedded Systems," Lecture Notes in Computer Science, Vol. 1717, pp. 122–134, Springer–Verlag, Berlin, 1999.) allows multiplication of complexity $N+1$ to be performed in $\mathbb{F}_{2^N}$ by working in a larger ring R of dimension $N+1$ over $\mathbb{F}_2$. In this paper we give a complete classification of all such rings and show that this construction is the only one which also has a certain useful permutability property.

Key Words: multiplicative complexity; finite field.

INTRODUCTION

The complexity of the multiplication operation in finite fields is of interest for both theoretical and practical reasons. More generally, let k be a field, and let R be a k-algebra with a finite basis

$$\mathscr{B} = \{x_1, x_2, \ldots, x_r\}$$

as a k-vector space. The multiplication law in R is determined by the relations

$$x_i x_j = \sum_{k=1}^{r} \lambda_{ij}^k x_k, \qquad 1 \le i, j, k \le r,$$

where the multipliers λ_{ij}^k are in k. The complexity of the multiplication law relative to the basis $\mathscr{B}$ is measured by the number of non-zero λ_{ij}^k's. More

1071-5797/00 $35.00

precisely, we define the *complexity* of the basis $\mathscr{B}$ to be

$$C(\mathscr{B}) = \frac{1}{r} \# \{(i,j,k) : \lambda_{ij}^k \neq 0\}.$$

For computational purposes, it is advantageous to choose a basis for R whose complexity is as small as possible. We define the *complexity* of R to be the smallest complexity among all k-bases of R,

$$C(R) = \min\{C(\mathscr{B}) : \mathscr{B} \text{ is a } k\text{-basis for } R\}.$$

For example, let $k = \mathbb{F}_2$ be the field with two elements, and let $R = \mathbb{F}_{2^N}$ be a finite field extension of k. Such fields are used extensively in cryptography, and there is a considerable literature devoted to the problem of efficiently implementing the multiplication operation in $\mathbb{F}_{2^N}$ in both hardware and software; see for example [1, 3, 4, 9, 11]. A particularly nice sort of basis for $\mathbb{F}_{2^N}/\mathbb{F}_2$ is a normal basis. Normal bases allow extremely rapid squaring of elements, and they have a nice "permutability" property which allows all of the λ_{ij}^k multipliers to be easily derived from the multipliers with $k = 1$. (We will discuss permutability in more detail below.) It is known that the complexity of a normal basis $\mathscr{B}$ for $\mathbb{F}_{2^N}/\mathbb{F}_2$ satisfies $C(\mathscr{B}) \geq 2N - 1$, and for certain fields it is possible to find a normal basis satisfying $C(\mathscr{B}) = 2N - 1$. Such bases are called "optimal normal bases," or ONB for short. See [1–3, 6–8] for further information about normal bases.

In [10] a new idea was introduced to perform computations in $\mathbb{F}_{2^N}$ with complexity smaller than $2N - 1$, while preserving many of the nice properties of (optimal) normal bases. Briefly, the idea is to write $\mathbb{F}_{2^N}$ as the quotient field of a ring R such that

$$\dim_{\mathbb{F}_2} R = N + 1 \qquad \text{and} \qquad C(R) = N + 1.$$

Thus storing elements of R requires only one more bit than for elements of $\mathbb{F}_{2^N}$, but multiplication in R is almost twice as fast as ONB multiplication in $\mathbb{F}_{2^N}$. Further, the rings constructed in [10] permit rapid squaring and have a permutability property similar to that of ONB. Thus high speed computations in $\mathbb{F}_{2^N}$ can be performed by first lifting elements to R, next doing all computations in R, and finally projecting the results back to $\mathbb{F}_{2^N}$.

A drawback of the construction in [10] is that it only works for certain fields $\mathbb{F}_{2^N}$, specifically fields for which $N + 1$ is prime and 2 is a primitive root modulo $N + 1$. A similar situation occurs for normal bases, where ONB are possible only for certain values of N. A complete classification of fields which

have an ONB is given in [2]. One of the main purposes of this paper is to provide a similar analysis for the construction in [10].

Thus let k be a finite field, let R be a k-algebra of dimension r, and suppose that R has a quotient field K of dimension $r-1$. In Theorem 4 we will give a complete classification of all such rings R with complexity satisfying $C(R) \leq r$. In particular, we will show that the only such rings having the permutability property are the ones already constructed in [10]. We will also prove a number of other properties of the complexity of rings, including the following:

- $C(R) \geq 1$ for all k-algebras R.
- $C(R) = 1$ if and only if $R = k^r$ with the usual product structure.
- If R is an integral domain, then $C(R) \geq \dim_k R$.
- If R is a finite field, then $C(R) = \dim_k R$ if and only if R is a Kummer extension of k (i.e., obtained by adjoining an rth root to k).

1. DEFINITIONS AND NOTATION

We set the following notation, which will remain fixed throughout the remainder of this paper:

k	a field
R	a finite k-algebra (i.e., R is a k-algebra that is finitely generated as a k-vector space)
$\mathscr{B}$	a basis $\{x_1, \ldots, x_r\}$ for R as a k-vector space.

The multiplication in R is determined by the products

$$x_i x_j = \sum_{k=1}^{r} \lambda_{ij}^k x_k, \qquad \lambda_{ij}^k \in k.$$

The *complexity* of the basis $\mathscr{B}$ is

$$C(\mathscr{B}) = \frac{1}{r} \# \{(i, j, k) : \lambda_{ij}^k \neq 0\},$$

and the *complexity of* R is the smallest complexity among all k-bases of R,

$$C(R) = \min\{C(\mathscr{B}) : \mathscr{B} \text{ is a } k\text{-basis for } R\}.$$

If the base field is not clear from the context, we will sometimes specify it by writing $C(R/k)$. For example, if k has a subfield k_0, then R will also be

a k_0-algebra. It is an interesting question to relate the complexities $C(R/k)$, $C(R/k_0)$, and $C(k/k_0)$.

Another useful property a basis may possess is a sort of symmetry whereby the r^3 multipliers λ_{ij}^k are determined by the r^2 multipliers λ_{ij}^1 using a simple transformation. We say that $\mathscr{B}$ is a *permutation basis* if there are permutations $\sigma_k, \tau_k \in \mathscr{S}_r$, $1 \le k \le r$, such that

$$\lambda_{ij}^k = \lambda_{\sigma_k(i),\tau_k(j)}^1 \qquad \text{for all } i, j, k.$$

In practical terms, this means that the circuitry used to compute the first coordinate of a product can be used to compute all of the coordinates merely by rearranging the order of the inputs. More precisely, if $a = \sum a_i x_i$ and $b = \sum b_j x_j$ and if $\mathscr{B}$ is a permutation basis as above, then

$$ab = \sum_{i,j,k=1}^{r} a_i b_j \lambda_{ij}^k = \sum_{k=1}^{r} \left(\sum_{i,j=1}^{r} a_{\sigma_k^{-1} i} b_{\tau_k^{-1} j} \lambda_{ij}^1 \right) x_k.$$

We also note that if $\mathscr{B}$ is a permutation basis, then its complexity is determined by the λ_{ij}^1's,

$$C(\mathscr{B}) = \#\{(i, j) : \lambda_{ij}^1 \neq 0\}.$$

Again for practical purposes, we want to work over a field. The idea is to start with a quotient field K of R, lift elements of K to elements of R, do all computations in R (where the complexity is hopefully small), and then move the result back to K. We define

$$\rho(R) = \dim_k R - \max\{\dim_k K : K \text{ is a quotient field of } R\}.$$

Thus we would like $\rho(R)$ to be small, which will say that R has a large quotient field. For example, $\rho(R) = 0$ if and only if R itself is a field. We also note that every quotient field K of R has the form $K \cong R/\mathfrak{M}$ for some maximal ideal $\mathfrak{M}$ of R, so an alternative definition for $\rho(R)$ is

$$\rho(R) = \min\{\dim_k \mathfrak{M} : \mathfrak{M} \text{ is a maximal ideal of } R\}.$$

2. EXAMPLES

In this section we give a number of examples illustrating the concepts from Section 1. We also prove some elementary properties of complexity.

EXAMPLE 1. Let $R = k^r$ with componentwise addition and multiplication, and let $\mathscr{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ be the standard basis, so $\mathbf{e}_i^2 = \mathbf{e}_i$ and $\mathbf{e}_i\mathbf{e}_j = 0$ for $i \neq j$. Then $\lambda_{ij}^k = 1$ if $i = j = k$ and $\lambda_{ij}^k = 0$ otherwise, so $C(\mathscr{B}) = 1$. Further, the largest quotient field of R is clearly k, so $\rho(R) = r - 1$. Thus R has no large quotient fields, but it is still an interesting example because it is the unique ring with the minimal possible complexity, as shown in the following proposition.

PROPOSITION 1. *Let R be any k-algebra of dimension r. Then its complexity satisfies $1 \leq C(R) \leq r^2$. Further, $C(R) = 1$ if and only if R is the ring $R = k^r$ described in example* 1.

Proof. The upper bound on $C(R)$ is trivial. Next let $\mathscr{B} = \{x_1, \ldots, x_r\}$ be a basis for R and write $1 \in R$ as a linear combination $1 = a_1 x_1 + \cdots + a_r x_r$ with $a_i \in k$. Multiplying by x_i gives

$$x_i = \sum_{k=1}^{r} \sum_{j=1}^{r} a_j \lambda_{ij}^k x_k,$$

so $\sum_j a_j \lambda_{ij}^i = 1$. This means that for every i there exists at least one j such that $\lambda_{ij}^i \neq 0$, so at least r of the λ_{ij}^k's are non-zero. This proves that $C(\mathscr{B}) \geq 1$, and hence $C(R) \geq 1$. Further, if $C(\mathscr{B}) = 1$, then for each i there is exactly one j with $\lambda_{ij}^i \neq 0$, say $\lambda_{ij(i)}^i \neq 0$, and every other $\lambda_{ij}^k = 0$. But by symmetry we have $\lambda_{ij}^i = \lambda_{ji}^i$, so we must have $j(i) = i$. In other words, $\lambda_{ii}^i \neq 0$, and every other $\lambda_{ij}^k = 0$, which means that $x_i^2 = \lambda_{ii}^i x_i$ for all $1 \leq i \leq r$. If we let $\mathbf{e}_i = (\lambda_{ii}^i)^{-1} x_i$, then $\mathbf{e}_i^2 = \mathbf{e}_i$, and we see that R is the ring described in Example 1.

EXAMPLE 2. Let $R = k[X]/(X^r)$. (R is an example of an Artinian local ring.) We take the natural basis $\mathscr{B} = \{1, X, X^2, \ldots, X^{r-1}\}$. The multiplication law is given by $X^i X^j = X^{i+j}$ if $i + j < r$, and $X^i X^j = 0$ if $i + j \geq r$, so

$$\lambda_{ij}^k = \begin{cases} 1 & \text{if } i + j = k < r, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to compute the complexity

$$C(\mathscr{B}) = \frac{1}{r} \sum_{\substack{0 \leq i, j < r \\ i+j<r}} 1 = \frac{r+1}{2}.$$

We thus see that the complexity may be non-integral. We also note that the only maximal ideal in R is the ideal XR, so the only quotient field of R is k. Hence $\rho(R) = r - 1$.

EXAMPLE 3. Let $A \in k$, $A \neq 0$, and consider the ring $R = k[X]/(X^r - A)$ with basis $\mathscr{B} = \{1, X, X^2, \ldots, X^{r-1}\}$. Then

$$X^i \cdot X^j = \begin{cases} X^{i+j} & \text{if } i + \mathrm{j} < r \\ AX^{i+j-r} & \text{if } i + j \geq r, \end{cases}$$

$$\lambda_{ij}^k = \begin{cases} 1 & \text{if } k = i + j, \\ A & \text{if } k = i + j - r, \\ 0 & \text{otherwise.} \end{cases}$$

The complexity of $\mathscr{B}$ is clearly

$$C(\mathscr{B}) = r,$$

since for each (i, j) there is exactly one k with $\lambda_{ij}^k \neq 0$.

Next factor $X^r - A = F_1 F_2 \cdots F_s$ into irreducible polynomials in $k[X]$, and let $d_i = \deg F_i$. Then $k[X]/(F_i)$ is a quotient field of R of dimension d_i, and these are the only quotient fields of R, so we see that

$$\rho(R) = r - \max d_i.$$

Of particular interest will be the case $A = 1$. If $A = 1$ and if the polynomial $\Phi(X) = X^{r-1} + X^{r-2} + \cdots + X + 1$ is irreducible in $k[X]$, then $\rho(R) = 1$. For example, if k is a finite field with q elements, then it is well known that $\Phi(X)$ is irreducible in $k[X]$ if and only if r is prime and q is a primitive root in $\mathbb{Z}/r\mathbb{Z}$. We also note that $\mathscr{B}$ is a permutation basis for R if and only if $A = 1$.

EXAMPLE 4. Let $k = \mathbb{F}_q$, and suppose that there is an element $\beta \in R$ such that the set $\mathscr{B} = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{r-1}}\}$ is a basis for R. A basis of this form is called a *normal basis for* R. If R is a field, then it is known that R has a normal basis, and further the complexity of any normal basis satisfies the inequality

$$C(\mathscr{B}) \geq 2r - 1.$$

(See, e.g., [1, 3, 6].) A basis satisfying $C(\mathscr{B}) = 2r - 1$ is called an *optimal normal basis*. See [2] for a complete description of all fields which possess an optimal normal basis. Normal bases over fields of characteristic 2 are especially nice, because the squaring operation is simply a cyclic shift of the coordinates; the use of an optimal normal basis makes multiplication as simple as possible. However, we observe that the squaring operation in the ring of Example 3 (in characteristic 2) is also a simple rearrangement of the coordinates, while the complexity of multiplication in Example 3 is about half the complexity of multiplication using an optimal normal basis.

EXAMPLE 5. Suppose that R_1 and R_2 are rings of dimension r_1 and r_2 over k, respectively, and let $\mathscr{B}_1$ and $\mathscr{B}_2$ be k-bases with $C(\mathscr{B}_i) = C(R_i)$ for $i = 1, 2$. Then the product ring $R = R_1 \times R_2$ of dimension $r = r_1 + r_2$ has a natural *product basis*

$$\mathscr{B} = \{(y, 0) : y \in \mathscr{B}_1\} \cup \{(0, z) : z \in \mathscr{B}_2\}.$$

Since $(y, 0)(0, z) = (0, 0)$, we can easily compute the complexity of the basis $\mathscr{B}$ by the formula

$$rC(\mathscr{B}) = r_1 C(\mathscr{B}_1) + r_2 C(\mathscr{B}_2) = r_1 C(R_1) + r_2 C(R_2).$$

It follows that

$$C(R_1 \times R_2) \leq \frac{r_1 C(R_1) + r_2 C(R_2)}{r_1 + r_2}.$$

Note that from a computational viewpoint, the use of a product basis for $R_1 \times R_2$ is quite uninteresting, since performing computations in $R_1 \times R_2$ using a product basis is exactly as complicated as doing the same computation in each of R_1 and R_2 individually. It is also easy to see that except for trivial cases, a product basis will not be a permutation basis.

EXAMPLE 6. The product basis of $R_1 \times R_2$ described in the previous example has the unpleasant property that it contains elements x_i, x_j with $x_i x_j = 0$. In the case where R_1 has dimension 1, that is, $R_1 = k$, we can eliminate this property by forming a *twisted product basis*

$$\mathscr{B} = \{(1, 1) : y \in \mathscr{B}_1\} \cup \{(0, z) : z \in \mathscr{B}_2\}.$$

The reason $\mathscr{B}$ is a basis is that we can write $(0, 1)$ as a k-linear combination of the elements $(0, z)$ with $z \in \mathscr{B}_2$, so the k-span of $\mathscr{B}$ also contains $(1, 1) - (0, 1) = (1, 0)$. It is easy to compute the complexity of $\mathscr{B}$ in terms of the complexity of $\mathscr{B}_2$. Precisely, let $x_1 = (1, 1)$, and let $x_i = (0, z_i)$ for $2 \leq i \leq r$, where $\mathscr{B}_2 = \{z_2, \ldots, z_r\}$. Then $x_1 x_i = x_i x_1 = x_i$ for all i, which gives $2r - 1$ non-zero λ_{ij}^k's. Further, if $2 \leq i, j \leq r$, then $x_i x_j = (0, z_i z_j)$ is given exactly by the linear combination which express $z_i z_j$ in terms of the basis $\mathscr{B}_2$. In other words, when $x_i x_j$ is written in terms of that basis $\mathscr{B}$, the element x_1 is not needed. This gives $r_2 C(R_2)$ non-zero λ_{ij}^k's. Hence

$$rC(R) = 2r - 1 + r_2 C(R_2).$$

Note that $r_2 = r - 1$, since we have assumed that $R_1 = k$ has dimension 1. This allows us to rewrite this formula as

$$C(R) - r = \left(1 - \frac{1}{r}\right)(C(R_2) - r_2).$$

In particular, $C(R_2) = r_2$ if and only $C(R) = r$. Thus the construction in this example will take a ring satisfying $C(R) = \dim_k R$ and produce a new ring with the same property, but of dimension one higher. Since $C(k) = \dim_k k = 1$, this proves that there exist rings of every dimension satisfying $C(R) = \dim_k R$.

EXAMPLE 7. Consider the ring $R = k[X]/(X^r - \alpha X - \beta)$ for some $\alpha, \beta \in k^*$ and the standard basis $\mathscr{B} = \{1, X, X^2, \ldots, X^{r-1}\}$. Then

$$X^i X^j = \begin{cases} X^{i+j} & \text{if } i + j < r, \\ \alpha X^{i+j-r+1} + \beta X^{i+j-r} & \text{if } i + j \geq r. \end{cases}$$

This gives a complexity of

$$rC(\mathscr{B}) = \#\{(i,j) : i + j < r\} + 2\#\{(i,j) : i + j \geq r\} = r\left(\frac{3r-1}{2}\right),$$

so $C(\mathscr{B}) = (3r - 1)/2$. Thus this is better than (say) a normal basis, since normal bases have complexity at least $2r - 1$. Of course, the basis in this example is not a permutation basis, nor is the squaring operation in R particularly easy, so an optimal normal basis has many advantages over the basis of this example.

EXAMPLE 8. Let $k = \mathbb{F}_2$, $\Phi(X) = X^r + X^{r-1} + \cdots + X + 1$, and let R be the ring $R = \mathbb{F}_2[X]/(\Phi(X))$. It is interesting to compute the complexity of the standard basis $\mathscr{B} = \{1, X, \ldots, X^{r-1}\}$ for R, since R sits quite naturally as a subring of $\mathbb{F}_2[X]/(X^{r+1} - 1)$, for which the standard basis has complexity $r + 1$. (We assume for simplicity that r is even.) It is not hard to check that multiplication in R is given by the rules

$$X^i X^j = \begin{cases} X^{i+j} & \text{if } i + j < r, \\ 1 + X + \cdots + X^{r-1} & \text{if } i + j = r, \\ X^{i+j-r-1} & \text{if } i + j > r. \end{cases}$$

There are thus r pairs (i, j) for which r of the λ_{ij}^k's are non-zero, and the remaining $r^2 - r$ pairs (i, j) have exactly one non-zero λ_{ij}^k, so

$$C(\mathscr{B}) = \frac{1}{r}(r^2 + r^2 - r) = 2r - 1.$$

Thus $\mathscr{B}$ has the same complexity as an optimal normal basis, which is approximately twice as large as the complexity of the ring of dimension one higher that contains R.

3. FIELDS OF LOW COMPLEXITY

In this section we consider the question of fields of low complexity. We begin more generally by giving an elementary lower bound for the complexity of an integral domain.

PROPOSITION 2. *Let R be a k-algebra of dimension r, and suppose that R is an integral domain. Then $C(R) \geq r$.*

Proof. Let $\mathscr{B} = \{x_1, \ldots, x_r\}$ be any k-basis for R. The assumption that R is an integral domain implies that $x_i x_j \neq 0$, so for each $1 \leq i, j \leq r$ there is at least one k such that $\lambda_{ij}^k \neq 0$. Hence there are at least r^2 non-zero λ_{ij}^k's so $C(\mathscr{B}) \geq r$. Since this is true for every basis, we have $C(R) \geq r$.

Proposition 2 says in particular that the complexity of a field is never less than its dimension. We now describe all field extensions of a finite field for which the complexity is exactly equal to the dimension. A slightly more elaborate argument can be used to give a similar classification for arbitrary base fields k, but we will leave this task for the interested reader.

THEOREM 3. *Let k be a finite field with q elements, and let K/k be a field extension of degree r. Then $C(K) = r$ if and only if the following two conditions are true*:

(i) *Every prime dividing r also divides $q - 1$.*

(ii) *Either $4 \nmid r$ or $4 \mid q - 1$.*

Further, if (i) and (ii) are true, then K is isomorphic to $k[X]/(X^r - A)$ for some $A \in k$ such that $X^r - A$ is irreducible in $k[X]$.

Remark. Theorem 3 says that $k = \mathbb{F}_2$ has no field extensions K with complexity $C(K) \leq \dim_k K$. However, if a computer has a special multiplier which makes multiplication in a larger field $k = \mathbb{F}_{2^a}$ very rapid, then the fields described in Theorem 3 may be useful. For example,

$$C(\mathbb{F}_{4^{3^n}}/\mathbb{F}_4) = 3^n$$

for all $n \geq 1$, and similarly for fields with 8^{7^n} elements over $\mathbb{F}_8$ and for fields with $16^{3^m 5^n}$ elements over $\mathbb{F}_{16}$. The idea of exploiting fast multiplication routines in smaller fields has been noted by a number of authors; see for example [11].

Question. In Example 7 we saw examples of fields K/k of dimension r with complexity $(3r-1)/2$. In view of Theorem 3, we might ask if $C(K) < (3r-1)/2$ implies that $K \cong k[X]/(X^r - A)$ for some $A \in k$?

Proof of Theorem 3. Let $\mathscr{B} = \{x_1, \ldots, x_r\}$ be any k-basis for K. By assumption, exactly r^2 of the λ_{ij}^k's are non-zero; and we know that for each i, j, at least one $\lambda_{ij}^k \neq 0$, since $x_i x_j \neq 0$. Hence for each i, j there is a unique k such that $\lambda_{ij}^k \neq 0$. In other words, the product of two basis elements always equals a non-zero multiple of a basis element, which implies that the set

$$\mathscr{B}^* =: k^*\mathscr{B} = \{ax : a \in k^*, x \in \mathscr{B}\}$$

is closed under multiplication.

We are going to prove that $\mathscr{B}^*$ is a subgroup of K^*. Take any $x \in \mathscr{B}^*$ and consider the powers $x, x^2, x^3, \ldots$ They are all in the finite set $\mathscr{B}^*$, so they must repeat, say $x^n = x^m$ with $n > m$. It follows that $1 = x^{n-m} \in \mathscr{B}^*$. Now take any $y \in \mathscr{B}^*$ and consider the multiplication map $\mathscr{B}^* \to \mathscr{B}^*$, $z \to yz$. It is injective, since K is a field, hence it is surjective, sine $\mathscr{B}^*$ is a finite set. In particular, there is some element $w \in \mathscr{B}^*$ such that $yw = 1$, so $\mathscr{B}^*$ contains a multiplicative inverse for each of its elements. This completes the proof that $\mathscr{B}^*$ is a subgroup of K^*.

The group K^* is cyclic (since K is a finite field), so $\mathscr{B}^*$ is also cyclic. Let $\alpha \in \mathscr{B}^*$ be a generator for $\mathscr{B}^*$. We are going to verify two claims:

(i) $1, \alpha, \ldots, \alpha^{r-1}$ are linearly independent over k, so they form a k-basis for K.

(ii) α^r is in k.

We prove (i) and (ii) simultaneously. Take the smallest value of $n \geq 1$ such that the set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly dependent over k. In particular, $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent, so $n \leq r$.

Each α^j is in $\mathscr{B}^*$, so we can write it as $\alpha^j = a_j x_{i(j)}$ for some $a_j \in k^*$ and some $1 \leq i(j) \leq r$. The set $\mathscr{B} = \{x_1, \ldots, x_r\}$ is k-linearly independent, so n must be the first power such that $i(n)$ repeats one of the previous $i(j)$'s But if $i(n) = i(j)$, then

$$\alpha^{n-j} = a_n a_j^{-1} \in k^*,$$

so $i(n-j) = i(0)$. Hence the minimality of n implies that $i(n) = i(0)$, and thus that $\alpha^n \in k^*$. It is immediate from this fact that every power of α is in the k-span of the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. But the powers of α give all of $\mathscr{B}^*$, so in

particular all of $\mathscr{B}$. Hence $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans K, so $n \geq r$. This proves that $n = r$, so we have produced a k-basis $\mathscr{B}' = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ for K with the property that $\alpha^r = A \in k$.

It follows that the map $k[X]/(X^r - A) \to K$ given by $X \to \alpha$ is a well-defined isomorphism, since the powers of α form a basis for K and both rings have dimension r over k. Further, the fact that K is a field means that the polynomial $X^r - A$ must be irreducible in $k[X]$.

We have now proven that if $C(K) = r$, then there is an irreducible polynomial $X^r - A$ in $k[X]$ such that K is isomorphic to $k[X]/(X^r - A)$. Conversely, if K has this form, then we observed in Example 3 that $C(K) = r$. It remains to figure out which fields K have this form.

The field K has q^r elements, and any two fields with q^r elements are isomorphic, so we are really asking for which values of r there is an irreducible polynomial of the form $X^r - A$ in $k[X]$. A basic result in field theory (see, e.g., [5, chapter VIII, Theorem 9.1]) says that $X^r - A$ is irreducible in $k[X]$ if an only if (i) for all primes $p | r$ we have $A \notin k^p$ (i.e., A is not a pth power in k), and (ii) if $4 | r$, then $A \notin -4k^4$.

The group k^* is cyclic of order $q - 1$. Suppose that we take A to be a generator for k^*. Then K is a pth power for every prime satisfying $p \nmid q - 1$, and A is not a pth power for every prime satisfying $p | q - 1$. Hence if $4 \nmid r$, we see that $X^r - A$ is irreducible if and only if every prime dividing r also divides $q - 1$. It remains to deal with the case $4 | r$.

So we assume now that $4 | r$, and we also suppose that every prime dividing r also divides $q - 1$. First, if also $4 | (q - 1)$, then we claim that one of A or A^{-1} is not in $-4k^4$. This is true because otherwise $A^2 = A/A^{-1} \in k^4$, contradicting the assumption that A generates k^*. It follows that one of $X^r - A$ or $X^r - A^{-1}$ is irreducible in $k[X]$, which covers the case $4 | (q - 1)$.

Next suppose that $4 \nmid (q - 1)$. This implies that $k^4 = k^2$ (note we may assume that k has odd characteristic). Hence condition (ii) is simply that $-A \notin k^2$, so conditions (i) and (ii) say that neither A nor $-A$ may be a square in k. However, the fact that $4 \nmid (q - 1)$ means that -1 is not a square in k, so these conditions are never simultaneously satisfied. This shows that if $4 | r$ and $4 \nmid (q - 1)$, then $X^r - A$ is never irreducible, which completes the proof of Theorem 3.

4. RINGS OF LOW COMPLEXITY

In this section we prove our main result, which is a complete classification of all rings R/k with low complexity $C(R) \leq \dim_k R$ and which have a quotient field of dimension $\dim_k R - 1$. In particular, we prove that if such an R has a permutation basis, then R is necessarily isomorphic to $k[X]/(X^r - 1)$.

THEOREM 4. *Let k be a finite with q elements, and let R be a k-algebra of dimension r satisfying*

$$\rho(R) = 1 \qquad \text{and} \qquad C(R) \le r.$$

Then R has one of the following forms:

(a) $R \cong k[X]/(X^r - 1)$, *where r is a prime and q is a primitive root modulo r. The basis $\mathscr{B} = \{1, X, X^2, \ldots, X^{r-1}\}$ is a permutation basis for R satisfying $C(\mathscr{B}) = C(R)$.*

(b) *There is a field K/k so that $R \cong k \times K$, and the basis $\mathscr{B}$* for R satisfying *$C(\mathscr{B}) = r$ is a twisted product basis as described in Example* 6. *Further, $C(K) = \dim_k K$, so in particular $K \cong k[X]/(X^{r-1} - A)$ is a field extension of the type described in Theorem* 3.

(c) *There is a field K/k so that $R \cong k \times K$, and the basis $\mathscr{B}$ for R satisfying $C(\mathscr{B}) \le r$ is a product basis as described in Example* 5.

(d) *$r = 2$ and $R \cong k[X]/(X^2)$.*

Only in case (*a*) *does R have a permutation basis $\mathscr{B}$ satisfying $C(\mathscr{B}) \le r$.*

Remark. The rings described in Theorem 4(a) are of particular interest for practical implementations of finite field arithmetic, especially in the case $k = \mathbb{F}_2$ and $R = \mathbb{F}_2 \times \mathbb{F}_{2^{r-1}}$. See [10] for further discussion.

Question. Theorems 3 and 4 describe fields and rings whose complexity lies on the edge of what is possible. It would be interesting to move away from that edge. For example, what do the rings with $\rho(R) = 2$ and $C(R) = \dim_k R$ look like? Similarly, what do fields with $C(K) = \dim_k K + 1$ look like?

Proof of Theorem 4. Let $K \cong R/\mathfrak{M}$ be a quotient field of R of maximal k-dimension, so $\mathfrak{M}$ is a maximal ideal of R and $\dim_k \mathfrak{M} = \rho(R) = 1$ by assumption. Let μ be a basis for $\mathfrak{M}$ as a k-vector space. Then

$$\mathfrak{M} = k \cdot \mu = R \cdot \mu. \tag{1}$$

We will make frequent use of this fact.

For example, consider the ideal

$$\mathfrak{p} = \{a \in R : a\mu = 0\}.$$

I claim that the natural inclusion $k \subset R$ followed by the projection $R \to R/\mathfrak{p}$ induces an isomorphism $k \cong R/\mathfrak{p}$. It is clear that the map is injective,since it is a homomorphism of k-algebras (in particular, $1 \to 1$) and k is a field. To see that it is surjective, take any $a \in R$. Then $a\mu \in \mathfrak{M} = k \cdot \mu$, so we can write $a\mu = \alpha\mu$ for some $\alpha \in k$. This implies that $a - \alpha \in \mathfrak{p}$, so a is equal to α in $R/\mathfrak{p}$.

This completes the verification that $k \cong R/\mathfrak{p}$. In particular, note that $\mathfrak{p}$ is a maximal ideal.

As a second example of the use of (1), since we know that $\mu^2 \in \mathfrak{M}$, it follows that $\mu^2 = \gamma\mu$ for some $\gamma \in k$. If $\gamma = 0$, then $\mu^2 = 0$, so μ is nilpotent. If $\gamma \neq 0$, then without loss of generality we may replace μ by $\gamma^{-1}\mu$, so $\mu^2 = \mu$ and μ is an idempotent. We consider these two cases separately.

We begin with the easier nilpotent case, so suppose that $\mu^2 = 0$. This implies that μ is in all maximal (indeed, in all prime) ideals. Thus $\mu \in \mathfrak{p}$, so $\mathfrak{M} = R\mu \subset \mathfrak{p}$, and the maximality of $\mathfrak{M}$ tells us that $\mathfrak{M} = \mathfrak{p}$. Comparing dimensions then gives

$$1 = \dim_k \mathfrak{M} = \dim_k \mathfrak{p} = \dim_k R - \dim_k k = r - 1,$$

so $r = 2$. Finally consider the k-algebra homomorphism $k[X]/(X^2) \to R$ induced by $X \to \mu$. It is well defined and injective since $\mu \neq 0$ and $\mu^2 = 0$, and both sides have k-dimension 2, so it is an isomorphism. This puts us in case (d) and completes the proof of Theorem 4 in the nilpotent case.

We now assume that μ is an idempotent, $\mu^2 = \mu$. As is well known,this means that R can be decomposed as a product of rings. In fact, this decomposition is given quite explicitly in our case by the map

$$R \xrightarrow{\sim} R/\mathfrak{p} \times R/\mathfrak{M} \cong k \times K.$$

(Note that $\mu \in \mathfrak{M}$ and $1 - \mu \in \mathfrak{p}$.) So for the remainder of the proof of Theorem 4 we will identify R with the product $k \times K$.

Take a k-basis $\mathscr{B} = \{x_1, \ldots, x_r\}$ for R satisfying $C(\mathscr{B}) = r$. Write each $x_i\mu = \gamma_i\mu$ for some $\gamma_i \in k$. If $\gamma_i \neq 0$, then we may replace x_i by $\gamma_i^{-1}x_i$, so we may assume that each basis element $x \in \mathscr{B}$ satisfies either $x\mu = 0$ or $x\mu = \mu$. Let $\mathscr{B}_0$ (respectively $\mathscr{B}_1$) be the elements $x \in \mathscr{B}$ with $x\mu = 0$ (respectively $x\mu = \mu$). We observe that $\mathscr{B}_1 \neq \emptyset$, since 1 is a linear combination of the elements of $\mathscr{B}$, so μ cannot annihilate all of $\mathscr{B}$.

We suppose now that $x_i x_j \neq 0$ for all $1 \leq i, j \leq r$. (We will deal with the other case later.) This implies that $C(R) \geq r$, since for each i, j there must be at least one non-zero λ_{ij}^k. Then our assumption that $C(R) \leq r$ implies that for each pair (i, j) there is a unique $k = k(i, j)$ such that $\lambda_{ij}^k \neq 0$. In other words, if $x, y \in \mathscr{B}$, then there is a unique $\lambda \in k^*$ and a unique $z \in \mathscr{B}$ such that $xy = \lambda z$.

We now consider the identification of R with $k \times K$. Under this identification, the element $\mu \in R$ corresponds to the pair (1, 0), so $\mathscr{B}_0$ consists of elements of the form $(0, u)$ and $\mathscr{B}_1$ consists of elements of the form $(1, u)$. Let $(1, u), (1, v) \in \mathscr{B}_1$; then $(1, u) \cdot (1, v) = (1, uv)$ is a k^*-multiple of an element of $\mathscr{B}$, so it must itself be an element of $\mathscr{B}_1$, since it certainly is not in $\mathscr{B}_0$. This

implies that the set

$$\{u : (1, u) \in \mathscr{B}_1\} \subset K$$

is closed under multiplication. Since K is a finite field, it follows that this set is a cyclic subgroup of K^*, say of order n and generated by some $w \in K^*$. In other words, we have shown that

$$\mathscr{B}_1 = \{(1, 1), (1, w), (1, w^2), \ldots, (1, w^{n-1})\}$$

for some $n \geq 1$ and some primitive nth root of unity $w \in K$.

Suppose first that $\mathscr{B}_0 \neq \emptyset$, and notice that although $\mathscr{B}_0$ need not be closed under multiplication, the set $k^*\mathscr{B}_0$ is closed. This implies that the same is true of the set

$$\{\alpha u : (0, u) \in \mathscr{B}_0,\ \alpha \in k^*\} \subset K. \tag{2}$$

We conclude that this set is a cyclic subgroup of K^*. In particular, $(0, 1) \in k^*\mathscr{B}_0$, so without loss of generality we may assume that $(0, 1) \in \mathscr{B}_0$.

Consider the product $(1, w)(0, 1) = (0, w)$. It is the product of two elements of $\mathscr{B}$, so it is a k-multiple of an element in $\mathscr{B}$, say $\alpha(0, w) \in \mathscr{B}$ with $\alpha \in k^*$. Then we have a k-linear relation

$$\alpha^{-1}(0, \alpha w) - (0, 1) - (1, w) + (1, 1) = (0, 0)$$

among the elements in the basis $\mathscr{B}$, so two or more of the basis elements in this identity must be identical. Hence either $w = 1$ or $w = \alpha^{-1}$. In any case, we see that $w \in k^*$. Then we observe that

$$(w - 1)(0, 1) + (1, 1) - (1, w) = (0, 0),$$

so the linear independence of elements in $\mathscr{B}$ tells us that $w = 1$. This proves that $\mathscr{B}_1 = \{(1, 1)\}$.

Let $\mathscr{B}'_0$ denote the projection of $\mathscr{B}_0$ to K; that is, $\mathscr{B}'_0$ is the set of second coordinates of the elements of $\mathscr{B}$. Since $\mathscr{B}_1$ consists of only a single element $\mathscr{B}_1 = \{(1, 1)\}$ and since $(0, 1) \in \mathscr{B}_0$, we see that $\mathscr{B}'_1$ must be a k-basis for K. This is true because it spans K and it contains at most $r - 1 = \dim_k K$ elements. This shows that

$$\mathscr{B} = \{(1, 1)\} \cup \{(0, z) : z \in \mathscr{B}'_0\}$$

is a twisted product basis for $R = k \times K$ as described in Example 6. Further,

$$C(\mathscr{B}_0') = r - 1 = \dim_k K,$$

so K/k is one of the fields described in Theorem 3. Thus we are in case (b) of Theorem 4.

We next suppose that $\mathscr{B}_0 = \emptyset$. This implies that $\mathscr{B}_1$ has r elements, so

$$\mathscr{B} = \mathscr{B}_1 = \{(1, 1), (1, w), (1, w^2), \ldots, (1, w^{r-1})\}$$

for some primitive rth root of unity $w \in K$. Consider the k-algebra homomorphism

$$k[X]/(X^r - 1) \to R, \qquad X \to (1, w).$$

It is well defined since $w^r = 1$, it is surjective since $\mathscr{B}$ is a k-basis for R, and hence it is an isomorphism since both sides are k-vector spaces of dimension r. Hence we are in case (a) of Theorem 4. In this case the field K in the decomposition $R \cong k \times K$ is isomorphic to $k[X]/(\Phi(X))$, where $\Phi(X)$ is the polynomial

$$\Phi(X) = X^{r-1} + X^{r-2} + \cdots + X + 1.$$

As is well known, $\Phi(X)$ is irreducible in the finite field with q element if and only if r is prime and q is a primitive root modulo r. This completes the proof of Theorem 4 in the case where $x_i x_j \neq 0$ for all basis elements $x_i, x_j \in \mathscr{B}$.

It remains to deal with the case where $x_i x_j = 0$ for some $1 \leq i, j \leq r$. Since $R \cong k \times K$, this means that (after relabeling) we have $x_1 = (\alpha, 0)$ and $x_2 = (0, w)$ for some $\alpha \in k^*$ and some $w \in K^*$. Replacing x_1 by $\alpha^{-1} x_1$, we may assume that $x_1 = \mu = (1, 0)$. For each i we write

$$x_i = (\alpha_i, w_i) \qquad \text{with } \alpha_i \in k \text{ and } w_i \in K.$$

We form a new basis $\bar{\mathscr{B}} = \{\bar{x}_1, \ldots, \bar{x}_r\}$ for R:

$$\bar{x}_i = \begin{cases} x_i = \mu = (1, 0) & \text{if } i = 1, \\ x_i - \alpha_i x_1 = (0, w_i) & \text{if } 2 \leq i \leq r. \end{cases}$$

We are going to compute the complexity of this new basis. First we observe that $\bar{x}_1 \bar{x}_1 = \bar{x}_1$ and that $\bar{x}_i \bar{x}_1 = 0$ for $2 \leq i \leq r$, so

$$\bar{\lambda}_{i1}^k = \bar{\lambda}_{1i}^k = \begin{cases} 1 & \text{if } i = k = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Next consider a product $\bar{x}_i\bar{x}_j$ with $2 \le i, j \le r$. Since $\bar{x}_i\bar{x}_j = (0, w_iw_j)$, and since $\bar{x}_1 = (1, 0)$ is the only element of $\bar{\mathscr{B}}$ with a non-zero first coordinate, we see that the product $\bar{x}_i\bar{x}_j$ must be a linear combination of the last $r-1$ basis elements $\bar{x}_2, \ldots, \bar{x}_r$. Multiplying out the product gives

$$\begin{aligned}\bar{x}_i\bar{x}_j &= (x_i - \alpha_i x_1)(x_j - \alpha_j x_1)\\ &= x_ix_j \underbrace{- \alpha_i x_jx_1 - \alpha_j x_ix_1 + \alpha_i\alpha_j x_1^2}_{\text{in } Rx_1, \text{ so in } kx_1}. \end{aligned} \tag{3}$$

Further,

$$\begin{aligned}x_ix_j = \sum_{k=1}^{r} \lambda_{ij}^k x_k &= \lambda_{ij}^1\bar{x}_1 + \sum_{k=2}^{r} \lambda_{ij}^k(\bar{x}_k - \alpha_k\bar{x}_1)\\ &= \left(\lambda_{ij}^1 - \sum_{k=2}^{r} \lambda_{ij}^k\alpha_k\right)\bar{x}_1 + \sum_{k=2}^{r} \lambda_{ij}^k\bar{x}_k. \end{aligned} \tag{4}$$

Comparing (3) and (4) and using the fact that $\bar{x}_i\bar{x}_j$ is a linear combination of $\bar{x}_2, \ldots, \bar{x}_r$, we see that

$$\bar{x}_i\bar{x}_j = \sum_{k=2}^{r} \lambda_{ij}^k\bar{x}_k.$$

This proves that for $2 \le i, j \le r$,

$$\bar{\lambda}_{ij}^k = \begin{cases} 0 & \text{if } k = 1,\\ \lambda_{ij}^k & \text{if } 2 \le k \le r. \end{cases}$$

We see from this that $C(\bar{\mathscr{B}}) \le C(\mathscr{B})$, with equality if and only if $x_1x_i = 0$ for all $2 \le i \le r$ and $\lambda_{ij}^1 = 0$ for all $2 \le i, j \le r$. However, the basis $\mathscr{B}$ was chosen to have minimal complexity among all k-bases of R, so we must have equality $C(\bar{\mathscr{B}}) = C(\mathscr{B})$. This implies that the basis $\mathscr{B}$ has the form

$$\mathscr{B} = \{(1, 0)\} \cup \{(0, w_2), \ldots, (0, w_r)\},$$

where $\mathscr{B}' = \{w_2, \ldots, w_r\}$ is a k-basis for K. In other words, $\mathscr{B}$ is a product basis for $k \times K$ as defined in Example 5, which puts us in case (d) of Theorem 4 and completes the classification part of the theorem.

Finally, it is easy to see that the bases in cases (b), (c), and (d) of Theorem 4 are not permutation bases. (Note that in case (b), the polynomial $X^{r-1} - A$ must be irreducible in $k[X]$, so in particular $A \ne 1$.) This completes the proof of Theorem 4.

Note Added in Proof. The fast multiplication method in [10] was earlier discovered by B. Ito and S. Tsujii, *Information and Computers* **83** (1989), 21–40. For related work, see G. Drolet, *IEEE Trans. Comput.* **47** (1998), 938–946 and J. K. Wolf, *Topics in Discrete Math.* **106/107** (1992), 497–502.

REFERENCES

1. G. B. Agnew, R. C. Mullin, and S. A. Vanstone, An implementation of elliptic curve cryptosystems over $F_{2^{155}}$, *IEEE J. Selected Areas Comm.* **11,** No. 5 (1993), 804–813.
2. S. Gao and H. W. Lenstra, Jr., Optimal normal bases, *Des. Codes Cryptogr.* **2** (1992), 315–323.
3. G. Harper, A. Menezes, and S. Vanstone, Public-key cryptosystems with very small key lengths, *in* "Advances in Cryptology—EUROCRYPT 92" (R. A. Rueppel. Ed.), Lecture Notes in Computer Science, Vol. 658, pp. 163–173, Springer–Verlag, New York, 1992.
4. Ç. K. Koç and T. Acar, Montgomery multiplication in GF(2^k), *Design, Codes Cryptogr.* **14** (1998), 57–69.
5. S. Lang, "Algebra," 2nd ed., Addison–Wesley, Reading, MA, 1984.
6. R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, Optimal normal bases in GF(p^n), *Discrete Appl. Math.* **22** (1988), 149–161.
7. J. Omura and J. Massey, "Computational Method and Apparaus for Finite Field Arithmetic," United States Patent 4587627 (May 6, 1986).
8. I. Onyszchuk, R. Mullin, and S. Vanstone, "Computational Method and Apparatus for Finite Field Multiplication," United States Patent 4745568 (May 17, 1988).
9. R. Schroeppel, S. O'Malley, H. Orman, and O. Spatscheck, Fast key exchange with elliptic curve systems, *in* "Advances in Cryptology—CRYPTO 95" (D. Coppersmith, Ed.), Lecture Notes in Computer Science, Vol. 973, pp. 43–56. Springer–Verlag, New York, 1995.
10. J. H. Silverman, Fast multiplication in finite fields GF(2^N), *in* "Cryptographic Hardware and Embedded Systems," Lecture Notes in Computer Science, Vol. 1717, pp. 122–134, Springer–Verlag, Berlin, 1999.
11. E. De Win, A. Bosselaers, S. Vandenberghe, P. De Gersem, and J. Vandewalle, A fast software implementation for arithmetic operations in GF(2^n), *in* "Advances in Cryptology—ASIACRYPT'96," Lecture Notes in Computer Science, Vol. 1163, pp. 65–76, Springer–Verlag, New York, 1996.